

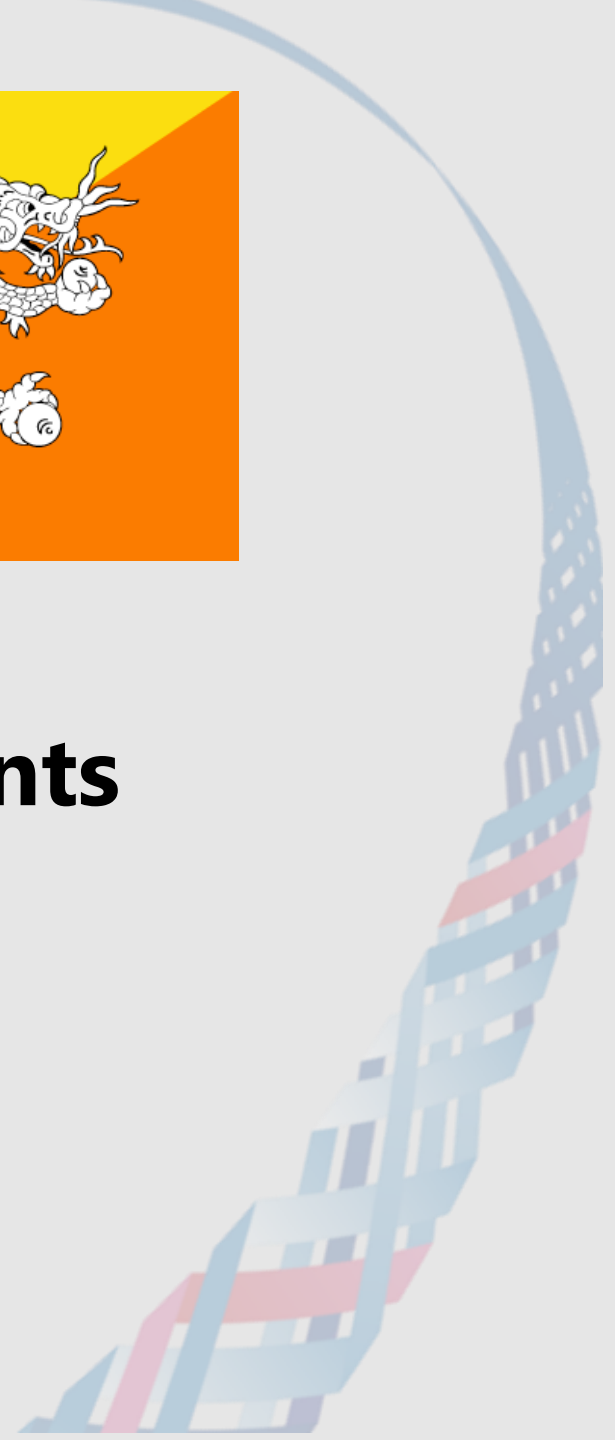


**Digital
transformation**



Health App Development (Reference) Non-Functional Requirements

April 2024



The “Non-Function Requirements” is to decide what is the working environment of APP

AIM

Content

Purpose of this document

- ✓ This document aims to define the requirements for the APP development

Positioning of this document

- ✓ This document aims to get the base understanding of Non-Functional Requirements, so that **the estimation of the proposal for the APP is clear**

Base understanding

- ✓ This Non-Functional Requirement for APP standard has been also based on the Digital Health Platform (DHP) that Bhutan government is creating. As the data of Health bank will be shared and connected through the DHP.
- ✓ Thus, please also make sure to also see the “04_Suppliment document_DHP Requirement Definition Documentv1.0_20230727(en)” of **DHP so that it is connected to DHP in smooth manner**

Overview of Non-Functional Requirements

The following is the overview of the Non-Functional requirements for APP.

	Topics	Content
Base Understanding	1 Usability and Accessibility	• Who are the users, what is the data volume, how many simultaneous access should be possible
	2 System method	• What is the overall policy on configuration of the information, structure of the information system
	3 Assumed scale	• What is the number of users, and volume of work (data)
System expectation	4 Performance	• What is the response time
	5 Reliability	• Availability of the app and confidentiality
	6 Scalability	• What is the assumed resource Scalability (CPU), Business volume growth
	7 Continuity	• What are the target values for continuity and measures related to continuity
	8 Security	• What are the authority requirements, risks and counter measures
	9 Information system	• What is software package configuration, network configurations, environment types

	Topics	Content
Project delivery	10 Testing	• What kind of testing is necessary
	11 Handover	• What is expected in handover
	12 Education	• What is expected in education
	13 Operation	• Operational management, monitoring, actual operation, period maintenance, evaluation
	14 Schedule	• Expected schedule

Please also look at the DHP Non-Functional requirements too, for reference to gain more understanding.

File: "04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)"

The APP, to be align with DHP, for non-functional requirements.

The comprehensiveness of the requirements are ensured by utilizing the "non-functional requirement grade*" used in system development in Japanese government offices.

Approach when considering the non-functional requirements

Step 1: Utilization of non-functional requirements grade *

Ensure comprehensiveness of requirements by utilizing "non-functional requirement grade*" used in system development in Japanese government offices
"Non-functional requirement grade*" is a comprehensive list of non-functional requirement items formulated by the Information-technology Promotion Agency (IPA). A document that defines each requirement level step by step

Step 2: Candidate selection of non-functional requirements

Patterns of non-functional requirements are defined as reference according to the degree of impact (human damage, economic loss, etc.) due to system failure, and non-functional requirements of the system that match the characteristics of this system are selected

Patterns according to impact degree

Step 3: Determine non-functional requirements in DHP

Determine the non-functional requirements in DHP from the non-functional requirements of the model system selected in step 2. For DHP-specific requirements, change the level of requirements where changes are necessary.

Determine non-functional requirements for DHP based on patterns

*References : Incorporated Administrative Agency Information-technology Promotion Agency (IPA) "Non-functional requirements grade 2018"

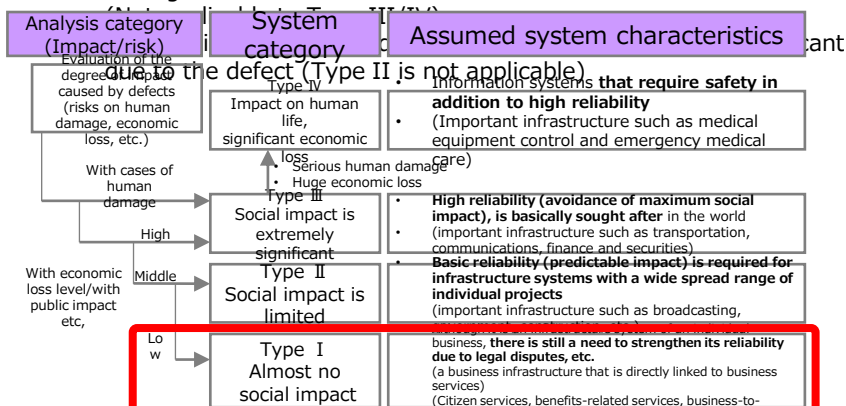
This health bank APP will be used by citizen and health workers, as data is mainly Personal Health Record(PHR) data, that data does not significantly impact human life nor economy, same as DHP, we have selected the requirement as "Type I Almost No Social impact".

However, if the Bhutan government decides on the development phase it could be increased in next phase contract with Bhutan government.

System category

- According to the degree of impact (human damage, economic loss, etc.) of a system failure, the category of the system is defined as shown in the following diagram *.
- As for DHP, it was selected based on the principle of "**Type I almost no social impact.**"

- Reason:
- Because it is not assumed that the defect will cause human damage



*References : Incorporated Administrative Agency Information-technology Promotion Agency (IPA) "Report of the critical infrastructure information system reliability study group - Overview"

Selection of candidates for non-functional requirements

- The non-functional requirements defined in a "almost no social impact" system are: (Red border)
- Determine the non-functional requirements for the DHP based on the content of the following non-functional requirements

Requirements	Property	System with almost no social impact	System with limited social impact	System with very significant social impact
Illustration of the model system				
General description of the model system		This type of system is used within a specific department of a company to a relatively limited extent. When its functions become degraded or unavailable, the specific department will be significantly affected while others will not. The system assumed here is a very small scale system that is open to the Internet.	This type of system provides the infrastructure for corporate activities. When its functions become degraded or unavailable, such corporate entities as well as external users including suppliers and customers will be significantly affected. The system assumed here is a mission-critical system that is restricted to a corporate network.	This type of system provides the infrastructure for people's lives and social/economical activities. When its functions become degraded or unavailable, both of these will be significantly affected. The system assumed here is an infrastructure that is used by the general public.
1	Availability	Uptime ratio Downtime of up to several days per year is accepted (99% uptime ratio).	Downtime of up to approximately an hour per year is accepted (99.99% uptime ratio).	Downtime of up to several minutes per year is accepted (99.999% uptime ratio).
2	Recovery objective	Restoration of data from a weekly backup will be the recovery objective when restoring data upon system recovery.	Restoration of data within one business day will be the recovery objective when restoring data upon system recovery.	Restoration of data to the point of outage within several hours will be the recovery objective when restoring data upon system recovery.
3	Large-scale disaster	The system is expected to be rebuilt in the event of a large-scale disaster.	The target recovery time is within a week in the event of a large-scale disaster.	Business continuity is required at a DR (Disaster Recovery) site in the event of a large-scale disaster. A backup center is established in anticipation of a large-scale disaster.
4	Performance and scalability	Performance objective A general performance objective is set, but is less important than other requirements.	A performance service level is specified.	A performance service level is specified.
5	Scalability	Scalability is not considered.	An expansion plan for the system is established.	An expansion plan for the system is established.
6	Operability and maintainability	Operating hours Service is provided during work hours only, and the system is not in operation during the nighttime.	A system outage window is secured between the completion of the nighttime batch process and the beginning of business operation.	The system operates 24/7 to provide non-interrupted service.
7	Backups	The administrator of the department manually backs up only necessary data.	A daily backup of the entire system is performed automatically.	A backup site (DR site) with all data synchronized with the operation site is established.
8	Operation monitoring	Active monitoring is performed using various types of hardware and software logs.	Each business function of the application is monitored to see whether they are operating normally.	Performance and resource usage is monitored to detect indications of failure.
9	Manuals	Manuals are created independently by the administrator of the department.	A maintenance manual is prepared along with the operation manual since service desk is established to carry out maintenance work.	The operation manual is customized in accordance with the operation rules of the data center.
10	Maintenance	Maintenance work is possible whenever necessary.	Shutting down the system for maintenance work is possible as long as operation during work hours is not affected.	All maintenance work is performed while the system is online.
11	Migratability	There are no rules for migration schemes (an agreement is reached based on the scheme proposed by the vendor).	Applications are proactively integrated and modified to streamline business operation. System takeover is performed all at once.	The system is migrated in phases to reduce risks.
12	Migration schedule	A sufficient number of days for migration is secured.	System outages due to migration are possible.	System outages due to migration shall be at minimum.
13	Equipment and data	Equipment and data are newly developed.	Equipment and data will have modifications.	There is migration of equipment and data. However, in order to maintain data consistency and compatibility with other systems, changes to the database structure are limited.
14	Security	Disclosure scope of critical assets There are no critical assets that require security measures. Critical assets refer to information assets that require high security, such as personal information, sensitive information, information with high profitability, etc.)	There are critical assets that require security measures, but connections are limited to specific parties.	There are critical assets that require security measures, and service is provided to an unspecified number of persons.
15	System environment and ecology	Restrictions There are no legal or regulatory restrictions, etc.	There are some legal and/or regulatory restrictions, etc.	There are legal and/or regulatory restrictions, etc.
16	Earthquake resistance	A minimum level of earthquake resistance is necessary.	A regular level of earthquake resistance is necessary.	A high level of earthquake resistance is necessary.

*References : Incorporated Administrative Agency Information-technology Promotion Agency (IPA) "Non-functional requirements grade 2018"

At DHP, it is not assumed that system failures will have a significant direct human or economic impact on operations. Thus, it has been selected as type1 "Almost no social impact".

System category

- According to the degree of impact (human damage, economic loss, etc.) of a system failure, the category of the system is defined as shown in the following diagram*.
- As for DHP, it was selected based on the principle of "**Type I almost no social impact**".
 - Reason:
 - Because it is not assumed that the defect will cause human damage (Not applicable to Type III/IV)
 - Because it is not assumed that the economic loss will be significant due to the defect (Type II is not applicable)

Analysis category (Impact/risk)

Evaluation of the degree of impact caused by defects (risks on human damage, economic loss, etc.)

With cases of human damage

High

Middle

Low

System category

Type IV
Impact on human life, significant economic loss

Type III
Social impact is extremely significant

Type II
Social impact is limited

**Type I
Almost no social impact**

Assumed system characteristics

- Information systems that require safety in addition to high reliability (Important infrastructure such as medical equipment control and emergency medical care)
- High reliability (avoidance of maximum social impact), is basically sought after in the world (important infrastructure such as transportation, communications, finance and securities)
- Basic reliability (predictable impact) is required for infrastructure systems with a wide spread range of individual projects (important infrastructure such as broadcasting, government, construction, etc.)
- Although it is an infrastructure system of an individual business, there is still a need to strengthen its reliability due to legal disputes, etc. (a business infrastructure that is directly linked to business services) (Citizen services, benefits-related services, business-to-business transactions, etc.)

*References : Incorporated Administrative Agency Information-technology Promotion Agency (IPA) "Report of the critical infrastructure information system reliability study group - Overview"

Selection of candidates for non-functional requirements

- The non-functional requirements defined in a "almost no social impact" system are: (Red border)
- Determine the non-functional requirements for the DHP based on the content of the following non-functional requirements*.

No.	Major category	Property	System with almost no social impact	System with limited social impact	System with very significant social impact
Illustration of the model system					
General description of the model system			The type of system is used within a specific department of a company to a relatively limited extent. When its functions become degraded or unavailable, the specific department will be significantly affected while others will not. The system assumed here is a very small scale system that is open to the internet.	This type of system provides the infrastructure for corporate activities. When its functions become degraded or unavailable, such corporate activities as well as external users including suppliers and customers will be significantly affected. The system assumed here is a mission-critical system that is restricted to a corporate network.	This type of system provides the infrastructure for people's lives and social/economical activities. When its functions become degraded or unavailable, both of these will be significantly affected. The system assumed here is an infrastructure that is used by the general public.
1	Availability	Uptime ratio	Downtime of up to several days per year is accepted (99% uptime ratio)	Downtime of up to approximately an hour per year is accepted (99.99% uptime ratio)	Downtime of up to several minutes per year is accepted (99.999% uptime ratio)
2	Recovery objective	Restoration of data from a weekly backup will be the recovery objective when restoring data upon system recovery.	Restoration of data from a weekly backup will be the recovery objective when restoring data upon system recovery.	Restoration of data within one business day will be the recovery objective when restoring data upon system recovery.	Restoration of data to the point of outage within several hours will be the recovery objective when restoring data upon system recovery.
3		Large-scale disaster	The system is expected to be rebuilt in the event of a large-scale disaster.	The target recovery time is within a week in the event of a large-scale disaster.	Business continuity is required at a DR (Disaster Recovery) site in the event of a large-scale disaster. A backup center is established in anticipation of a large-scale disaster.
4	Performance and scalability	Performance objective	A general performance objective is set, but is less important than other requirements.	A performance service level is specified.	A performance service level is specified.
5		Scalability	Scalability is not considered.	An expansion plan for the system is established.	An expansion plan for the system is established.
6	Operability and maintainability	Operating hours	Service is provided during work hours only, and the system is not in operation during the nighttime.	A system outage window is secured between the completion of the nighttime batch process and the beginning of business operation.	The system operates 24/7 to provide non-interrupted service.
7		Backups	The administrator of the department manually backs up only necessary data.	A daily backup of the entire system is performed automatically.	A backup site (DR site) with all data synchronized with the operation site is established.
8	Operation monitoring	Active monitoring is performed using various types of hardware and software logs.	Each business function of the application is monitored to see whether they are operating normally.	Performance and resource usage is monitored to detect indications of failure.	
9	Manuals	Manuals are created independently by the administrator of the department.	A maintenance manual is prepared along with the operation manual since service desk is established to carry out maintenance work.	The operation manual is customized in accordance with the operation rules of the data center.	
10	Maintenance	Maintenance work is possible whenever necessary.	Shutting down the system for maintenance work is possible as long as operation during work hours is not affected.	All maintenance work is performed while the system is online.	
11	Migratability	Migration scheme specification	There are no rules for migration schemes (an agreement is reached based on the scheme proposed by the vendor).	Applications are proactively integrated and modified to streamline business operation. System takeover is performed all at once.	The system is migrated in phases to reduce risks.
12		Migration schedule	A sufficient number of days for migration is secured.	System outages due to migration are possible.	System outages due to migration shall be at minimum.
13	Equipment and data	Equipment and data are newly developed.	Equipment and data will have modifications.	There is migration of equipment and data. However, in order to maintain data consistency and compatibility with other systems, changes to the database structure are limited.	
14	Security	Disclosure scope of critical assets	There are no critical assets that require security measures. Critical assets refer to information assets that require high security, such as personal information, sensitive information, information with high volatility, etc.)	There are critical assets that require security measures, but connections are limited to specific parties.	There are critical assets that require security measures, and service is provided to an unspecified number of persons.
15	System environment and ecology	Restrictions	There are no legal or regulatory restrictions, etc.	There are some legal and/or regulatory restrictions, etc.	There are legal and/or regulatory restrictions, etc.
16	Earthquake resistance	Earthquake resistance	A minimum level of earthquake resistance is necessary.	A regular level of earthquake resistance is necessary.	A high level of earthquake resistance is necessary.

*References : Incorporated Administrative Agency Information-technology Promotion Agency (IPA) "Non-functional requirements grade 2018"

(Reference) List of non-functional requirements (Type I)

Non-functional requirements for "Type I almost no social impact" are shown in annex "Annex 04_Non-functional requirements list".

No.	Major cate.	Middle cate.	Minor category	Minor category descriptive	Metric	Level					Impact on ration tests	Notes	System with almost no social impact		System with limited social impact		System with very significant social impact					
						0	1	2	3	4			5	Selecte	Selection condition	Selected	Selection condition	Selected	Selection condition			
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	Operating hours (normal)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours	X	<p>[Overlapping Item] C.1.1.1. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability".</p> <p>[Metric] "Operating hours" refers to the time periods when the system is operational, including online and batch processing.</p> <p>[Level] The times in parentheses "[]" are examples for each level. They are not to be used as level selection conditions. "Not specified" refers to a system not having specified service hours, and is envisioned essentially for cases where the system is shut down and started up as necessary by users (Ex: Backup systems prepared for failure recovery, development and validation on systems, etc.) "During business hours" and "Outage only at night" are envisioned for general business usage, and the times provided as examples should be read as examples only, and modified as appropriate for systems with different operating hours. "Possible outage" refers to time periods where the system may possibly be shut down, not where it must be shut down. "Uninterrupted 24 hours" also includes cases where batch processes must be executed when the system is not involved in online business, and which therefore require that the system not be shut down.</p>	2	Outage only at night (9:00 to 21:00)	No businesses are done during nighttime and thus system shutdown is possible. [] Business is performed during a more limited amount of operating hours. [+] When considering uninterrupted 24 hour operation or only short interruptions for reboot processing, etc.	4	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hour operation is not necessary, but continual operation to the extent as possible is desired. [] Long periods of operation outage, such as not permitting access at night [+] Uninterrupted 24 hour operation	5	Uninterrupted 24 hours	There are no time periods during which the system can be shut down. [] There is a regular period during each day when operation can be shut down.
A.1.1.2					Operating hours (specific days)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hours	X	<p>[Overlapping Item] C.1.1.2. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability".</p> <p>[Metric] "Specific days" refer to weekends, holidays, the end/start of months, and other days whose schedule is defined as differing from the normal operation schedule. If there are multiple specific days, their level values must be made consistent (Ex: "Monday to Friday" is level 2, but "Saturday and Sunday" are level 0. "Normally, the level is 5, but the system is rebooted on the first of each month, so on that day, the level is 3"). In addition to user holidays, vendor holidays must also be recognized as specific days, and an operation and maintenance structure, etc. must be established accordingly.</p>	0	Not specified	There are no specific days with operating hours that differ from normal days. [+] There are specific days with operating hours that differ from normal days, such as backup operations performed on weekends/holidays.	2	During business hours (9:00 to 17:00)	During weekends, only backup operations are performed, so the system is shut down at night. [] There are no weekend backups or batch processing, etc. and operation is stopped on weekends/holidays. [+] The system is used for business by employees who come in on weekends/holidays, so the system operates on weekends/holidays as well.	5	Uninterrupted 24 hours	There are no time periods during which the system can be shut down. [+] There are regularly scheduled days when operation is stopped.
A.1.1.3					Existence of planned system shutdown	Possible planned system shutdown (operation schedule can be changed)	Possible planned system shutdown (operation schedule cannot be changed)	No planned system shutdown				X	<p>[Overlapping Item] C.2.1.1. "Existence of planned system shutdown" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability".</p> <p>[Impact on Operation Costs] When there are planned system shutdown, operational costs may increase due to pre-shutdown backups and the preparation of procedures in accordance with the system configuration.</p>	0	Possible planned system shutdown (operation schedule can be changed)	System shutdown is possible if consensus is gained in advance. [+] When it is sufficient with only outages during non-operating hours	1	Possible planned system shutdown (operation schedule cannot be changed)	Uninterrupted 24 hour operation is not necessary. There are hours during which outage is possible, and planned outages are possible. [] There are no times within the operation schedule during which outages are possible, but outages possible if coordinated in advance. [+] When uninterrupted 24 hour operation is required	2	No planned system shutdown	There are no time periods during which the system can be shut down. [] There are times within the operation schedule during which outages are possible, and there is a need for planned system shutdowns.
A.1.2.1			Business continuity	Business scope and conditions required to ensure availability	Affected business scope	Internal batch related businesses	Internal online businesses	All internal businesses	External batch related businesses	External online businesses	All businesses	X	<p>[Metric] The "affected business scope" here refers to the scope which is used for uptime ratio calculation.</p> <p>[Level] "Internal" refers to closed (business) processing within the system. "External" refers to (business) processing which requires coordination with other systems.</p>	2	All internal businesses	The primary businesses handled by the system are internal businesses, and one of the system operation conditions is that all internal businesses are operational. [+] There are also externally provided businesses, which are considered essential.	3	External batch related businesses	The primary businesses handled by the system are external batch processing businesses, and one of the system operation conditions is that all internal businesses and external batch processing businesses are operational. [] There are no externally provided businesses. [+] Real-time processing with external entities is required for business continuity.	4	External online businesses	The primary businesses handled by the system are real-time processing with external entities, and one of the conditions of system operation is that external online businesses are operational. [] Real-time processing with external entities is not required for business continuity.
A.1.2.2					Service switchover time	24 hours or longer	Less than 24 hours	Less than 2 hours	Less than 60 minutes	Less than 10 minutes	Less than 60 seconds	X	<p>[Metric] "Service switchover time" refers to the amount of time necessary for a system which has suffered a possible failure (such as temporary business interruption due to hardware failures, etc.) to resume business by taking response measures (for example, performing server switchover in a clustered system).</p> <p>[Impact on Operation Costs] The longer the permitted interruption time, the ratio of manual response as recovery measures will be greater than automatic system response measure implementation, impacting operation costs.</p>	1	Less than 24 hours	There is no business provided to external entities, and a down time of approximately 1 day is acceptable. [] Failure countermeasures are not necessary. [+] Service switchover has an impact. (Consider the amount of time that interruption is acceptable based on the impact.)	3	Less than 60 minutes	There are online businesses with external entities, but interruptions of several dozen minutes are acceptable. [+] Service switchover has an impact on the online businesses. (Consider the amount of time that interruption is acceptable based on the impact.)	5	Less than 60 seconds	The system must provide real-time response, so instant recovery from system outages is required. [] Business interruption of up to 1 hour is acceptable.

List of Non-functional Requirements

Below is a list of minimum non-functional requirements for digital platforms and app development (based on other APP reference)

1. Usability and Accessibility Matters

- 1.1 Types of users of information system
- 1.2 Usability Requirements
- 1.3 Accessibility Requirements

2. System method matters

- 2.1 Overall policy on the configuration of information systems
- 2.2 Overall structure of information systems

3. Matters relating to scale

- 3.1 Number of locations
- 3.2 Volume of work
- 3.3 Number of locations

4. Performance matters

- 4.1 Response time (response time, turnaround time, server processing time)

5. Reliability matters

- 5.1 Availability requirements
- 5.2 Confidentiality Requirements

6. Scalability matters:

7. Continuity matters:

- 7.1 Target values for continuity
- 7.2 Measures related to continuity

8. Information Security Matters

- 8.1 Basics
- 8.2 Authority requirements
- 8.3 Overview of Risks and counter measures
- 8.4 Information security measures requirements

9. Information system and operation requirements

- 9.1 Software Package Configuration
- 9.2 Network Configuration
- 9.3 Environment Types

- 9.4 Req for the implementation of the environment

10. Matters relating to testing

- 10.1 Testing Common Process Requirements
- 10.2 Test Environment Requirements
- 10.3 Test Data Requirements
- 10.4 Types of testing
- 10.5 Foundation Testing Requirements
- 10.6 Unit Testing Requirements
- 10.7 Coupled Testing Requirements
- 10.8 Comprehensive Testing Requirements
- 10.9 Acceptance testing support requirements

11. Matters on Handover:

- 1.1 Handover to the common Operation Management contractor and the next application software maintenance contractor

12. Matters relating to Education

- 12.1 Basic requirements for education
- 12.2 Requirements regarding educational contents
- 12.3 Other educational Requirements

13. Matters relating to Operation:

- 13.1 Common Requirements
- 13.2 Operational Management and Monitoring requirements
- 13.3 Evaluation and improvement of actual operations
- 13.4 Periodic maintenance requirements
- 13.5 Maintenance System

Defining the availability of non-functional requirements for the health service app development

S.No	Non-functional Requirements	Required in App? (Yes/No)	Availability in DHP (Yes/No)	Details for the app as per DHP NFR
1.1	Types of users of information system	Yes	Yes	<ul style="list-style-type: none"> As per 4 use-cases - Citizens, Government, Health Professionals, Health Staff
1.2	Usability Requirements	Yes	Yes	<p>Data Volume –</p> <ul style="list-style-type: none"> Number of users: MAX 750,000 Simultaneous access: PoC 3000 (expected), Development phase Min 60000, Likely 350000, Max 750,000 Data volume: Key data is clear <p>Data details on excel sheet "03_FunctionalList_Draft Data Category of Data Bank_V1.0_(JICA_BhutanDX)" tab "DataVolumeCalculationParameter"</p>
1.3	Accessibility Requirements	Yes	Yes	<ul style="list-style-type: none"> Simultaneous access: Unspecified number of accesses No. of health facilities – 184 (during development) No. of health facilities – 2 or 3 (during PoC phase) Max simultaneous access for PoC – 3000 (individuals) Reference also to Page 43 (04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)) Access Line – Application/service to DHP (API) security requirements, refer to page 63 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)

The basic policies for data volume and scalability are shown below.

Data volume/scalability requirements	
Data volume	<p>Operation processing volume</p> <ul style="list-style-type: none"> • Number of users: MAX 750,000 • Simultaneous access: • PoC 3000 , Development phase Min 60000, Likely 350000, Max 750,000 • Data volume: Key data is clear • Number of online requests: Clear main process • Batch processing number: Clear for each processing unit
Scalability	<p>Business volume growth</p> <ul style="list-style-type: none"> • Secure One point two times the performance based on the amount of work currently assumed • Since this is the cloud, do not reserve excessive resources in the future
	<p>Resource scalability</p> <ul style="list-style-type: none"> • CPU utilization: 80% • CPU scalability: No scalability requirements • Memory utilization: 80% • Memory scalability: No scalability requirements



Basic policy for data volume and scalability	
Data volume	<ul style="list-style-type: none"> • Consider the peak load during operation so that the service can be continuously provided even if the business load increases during operation of this system. • Implement the sizing according to temporary high load. If it becomes higher than the peak sizing during operation, it becomes an excessive specification. Therefore, performance is determined based on peak processing during operation.
Scalability	<ul style="list-style-type: none"> • The scalability is arranged from the following viewpoints so that the performance can be expanded when the system is expanded in the future. <ol style="list-style-type: none"> ① Use a service that can be expanded according to the amount of cloud service used ② Servers and virtual machines whose resources are predetermined are expanded by the following method. <ol style="list-style-type: none"> (2) -1. Scale up: Add memory/hard disk (2) -2. Scale out: Increase the number of servers

3-1 . Functional requirements 2 . Functional requirements

(1) Authentication (application logon)

The users are citizens and professionals (medical workers such as care workers). Based on the use cases by each user, citizens use NDI as a function of authentication/identity verification (CID will be extracted). Professionals use the authentication function provided by DHP.

	APP user	Usage case	Authentication method	Reason for choosing authentication method
(1)	Citizens	<ul style="list-style-type: none"> With DHP, citizens agree to provide health data and utilize their own health data. Identity verification is important when agreeing to provide data and using one's data. 	Use NDI authentication function (Get CID)	<ul style="list-style-type: none"> By using the NDI authentication function provided by the Government of Bhutan, it is possible to ensure a more secure environment. Since NID, which is a national ID, is used, there is no need to hold multiple IDs.
(2)	Professionals (medical workers such as care workers)	<ul style="list-style-type: none"> With DHP, professionals (medical workers such as care workers) define the data that can be used based on their roles, and refer to patient data. Roles of professionals (medical workers such as care workers) are defined in each application and users are registered. 	Provide authentication function in DHP	<ul style="list-style-type: none"> Since the data that can be used as "other than" the citizen is defined based on the role, it is necessary to perform authentication with a mechanism different from NDI. Therefore, DHP provides an authentication function.

3-1 . Functional requirements 2 . Functional requirements

(5) Data access control

Based on the consent of the citizens, APP needs to identify users who have access to each data provided. APP users are classified into "citizens" and "professionals (medical workers such as care workers)". "Citizens" can use their own data that they have consented to, and "professionals" can use data that citizens have consented to provide based on their role.

		Category of access control	
		Role-based (Limit available data based on user role. Like, care workers can only view data for their own patients)	Consent-based (Define the data that can be used by citizens by purpose of use and by Bank)
User category	Citizens (Use own health data)	Citizens should be able to use their own healthcare data. (Define and control roles in DHP)	Only data that is allowed to be used by the application that accesses it with the Consent & Data Access function can be used.
	Professionals (medical workers such as care workers) (Using health data of patients, etc.)	Based on the role in charge, only the data necessary for the execution of work can be viewed by professionals of healthcare workers such as care workers. (The role is defined and controlled by the application)	Only data that is allowed to be used by the application that accesses it with the Consent & Data Access function can be used.

The basic policy for the data retention period is shown below.

Data retention requirements

Retention period

- Data retention period is 10 years
After the 1th year, delete the data that was registered 1 years ago and maintain the data saved for the last 10 years.



Basic policy on data retention period

- Summarize the retention period required for the data necessary for the system so that past data can be referenced for investigation of the cause and audit when a failure occurs

S.No.	Non-functional Requirements	Required in App? (Yes/No)	Availability in DHP (Yes/No)	Details
2 System method matters				
2.1	Overall policy on the configuration of information systems	Yes	Yes	Security Requirements – System configuration management - When incidents occur, manage the configuration and operational condition of information systems, as well as enable tracking and investigation of causes and selection of relevant countermeasures (Page 66) of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)
2.2	Overall structure of information systems	Yes	Yes	System configuration diagram (Pg 75) of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)
3 Matters relating to scale				
3.1	Number of processes	Yes	Yes	<ul style="list-style-type: none"> Processes as defined in the to-be journey, step and function list No. of APIs needed to connect data from Health Bank to DHP – at least 13
3.2	Number of users	Yes	Yes	Maximum up to 7,50,000 users defined in DHP data type description
3.3	Volume of work	Yes	Yes	Data volume and scalability requirements given in DHP Operation and maintenance requirements. Volume of business which have an effect on performance and scalability. Consensus is to be based on envisioned system operation. Instead of selecting a single value for each metric, intended system operation hours, seasonal factors, and the like must also be considered.

S.No	Non-functional Requirements	Required in App? (Yes/No)	Availability in DHP (Yes/No)	Details
4 Performance Matters				
4.1	Response time (response time, turnaround time, server processing time)	Yes	Yes	<ul style="list-style-type: none"> Case Urgency and response time for developers - General guidance: Within 24 hours System failure: Within 12 hours (Page 60 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)) Disaster recovery requirements describe the incident response time
5 Reliability matters				
5.1	Availability requirements	Yes	Yes	<ul style="list-style-type: none"> Information regarding system operating hours and operation outage Operating hours - Level 1 - Outage only at night (9:00 to 21:00)
5.2	Confidentiality requirements	Yes	Yes	<ul style="list-style-type: none"> Data confidentiality under security requirements – assuming no use of portable media (Page 66 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en))

S.No.	Non-functional Requirements	Required in App (Yes/No)	Availability in DHP (Yes/No)	Details
6	Scalability matters	Yes	Yes	<p>Resource Scalability</p> <ul style="list-style-type: none"> • CPU utilization: 80% • CPU scalability: No scalability requirements • Memory utilization: 80% • Memory scalability: No scalability requirements <p>Business volume growth</p> <ul style="list-style-type: none"> • Secure One point two times the performance based on the amount of work currently assumed • Since this is the cloud, do not reserve excessive resources in the future

S.No.	Non-functional Requirements	Required in App (Yes/No)	Availability in DHP (Yes/No)	Details
7 Continuity Matters				
7.1	Target values for continuity	Yes	Yes	<ul style="list-style-type: none"> Target users - document is intended for those involved in PoC, design, development, operation and maintenance of DHP. Specifically, the system manager of the Government of Bhutan involved in DHP development. The target readers are the GovTech personnel responsible for design, development, operation and maintenance, and GDC personnel in-charge for design, development, operation and maintenance. (page 4 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)) Performance target Migration target data Target recovery level - This metric is the target recovery time in the event of a large-scale disaster. Large-scale disasters refer to damage caused by fires and natural hazards such as earthquakes, as well as man-made damage that are accidental or intentional, which cause extensive damage to the system, or make it difficult to recover the system because lifelines such as power are interrupted. Resumption within several months
7.2	Measures related to continuity	Yes	Yes	<ul style="list-style-type: none"> Business continuity plan Supported by tests that include simulations of various scenarios. During and after testing, AWS documents team and process responses, corrective actions, and lessons learned for continuous improvement. Pandemic response We incorporate pandemic response policies and procedures into our disaster recovery plans to prepare for a rapid response to the threat of an infectious disease outbreak.

S.No	Non-functional Requirements	Required for App Development (Yes/No)	Availability in DHP (Yes/No)	Details
8 Information Security Matters				
8.1	Basics	Yes	Yes	Mentioned under security requirements
8.2	Authority Requirements	Yes	Yes	<ul style="list-style-type: none"> • This item is for confirming whether or not there are information security related organizational policies, rules, laws, guidelines, etc., which must be observed by users. • In the event that there are rules, etc. to be observed, measures must be considered to ensure that there are no conflicts with said regulations, etc. • Information security policy • Act Concerning the Prohibition of Unauthorized Computer Access • Personal Information Protection Law • Electronic Signature Law • Provider Responsibility Law • Act on Regulation of Transmission of Specified Electronic Mail • Sarbanes-Oxley Act • Basic Law for Building an Advanced Info-Communications Network • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISMA • FISC • PCI DSS • PrivacyMark System • TRUSTe etc. (* The above examples are mainly Japanese laws, systems, etc.)
8.3	Overview of Risks and counter measures	Yes	Yes	<ul style="list-style-type: none"> • Counter measures under fraud monitoring
8.4	Information Security measures requirements	Yes	Yes	<ul style="list-style-type: none"> • Mentioned under security requirements, information security compliances

S.No	Non-functional Requirements	Required for App Development (Yes/No)	Availability in DHP (Yes/No)	Details
9 Information System Operating Requirements				
9.1	Software Package Configuration	Yes	Yes	<ul style="list-style-type: none"> Cloud environment related requirements API Management (Page 18 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en)) - API Gateway, API aggregation and Monitoring, API Manager
9.2	Network Configuration	Yes	Yes	<p>System configuration diagram DHP (Page 75 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en))</p> <p>Step :</p> <ol style="list-style-type: none"> The user makes a REST API call from a Web app or mobile app, which is passed to DHP via Internet Gateway. AWS API Gateway uses Lambda Authorizer to validate the token using the public key from Secrets Manager. If successful, fetch the relevant policy from DynamoDB . API Gateway evaluates the policy received from Authorizer and accesses the associated Lambda function Each Lambda function performs different CRUD operations against different AWS RDS databases. <p>(From Excel sheet) Networking requirement - Requirements to maintain the requested service when a failure occurs on equipment, such as routers or switches, which make up a network.</p>
9.3	Environment Types	Yes	Yes	<ul style="list-style-type: none"> With reference to AWS Data center design PoC Environment, Developer environment, Verification Environment and
9.4	Requirements for the implementation of the environment	Yes	Yes	<ul style="list-style-type: none"> System configuration implementation policy. When incidents occur, manage the configuration and operational condition of information systems, as well as enable tracking and investigation of causes and selection of relevant countermeasures. (Page 76 of 04_Suppliment document_ DHP Requirement Definition Documentv1.0_20230727(en))

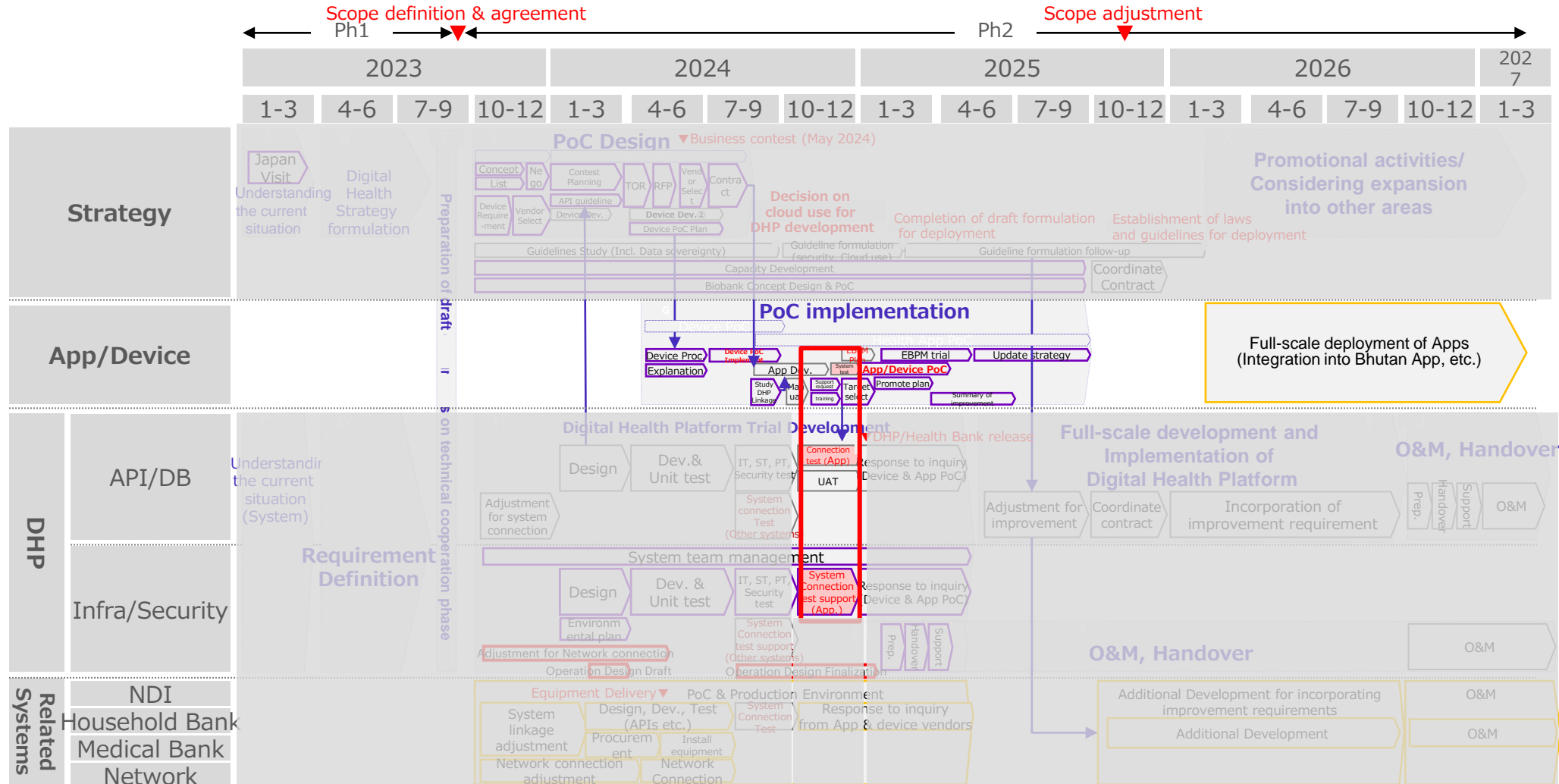
S.No	Non-functional Requirements	Required in App Dev> (Yes/No)	Availability in DHP (Yes/No)	Details
10 Matters related to testing				
10.1	Common Requirements for Testing Process (excluding acceptance testing)	Yes	Yes	<ul style="list-style-type: none"> Testing scenarios to be included for use cases A,B,C. test schedules to be added and the same to be mentioned in the proposal schedule as well. Testing scenarios to be clearly stated on the methodology such as the mock app of android and iOS or through an online testing environment. The developed App should be usable for the PoC
10.2	Test data requirements	Yes	Yes/No	<ul style="list-style-type: none"> Mentioned under environment purpose - Use test data instead of production data in POC, Development and Verification environment
10.3	Test Environment Requirements	Yes	Yes	<ul style="list-style-type: none"> Mentioned under environment requirements - POC environment, Development environment, verification environment, production requirement
10.4	Test Types	Yes	No	<ul style="list-style-type: none"> Scenario (Business Pattern) Performance testing at least prior to PoC, it should ensure it doesn't crash in less than 10 people simultaneously working. (Also, at the very least, it is necessary to confirm that the process will not be slowed down by the expected number of users at 3000 in the PoC).Interface test (number of data to be linked) for DHP test (Even if it is all in the API, is the data linked correctly?))
10.5	Fundamental Testing Requirements	Yes	No	
10.6	Unit Testing Requirements	Yes	Yes	<ul style="list-style-type: none"> Unit testing in development requirement
10.7	Coupled Testing Requirements	Yes	No	
10.8	Comprehensive testing requirements (including regression testing)	Yes	No	
10.9	Acceptance testing support requirements	Yes	No	<ul style="list-style-type: none"> Since it will be used by the hospital in PoC, the procedure manual on the vendor side should be included Once you've made it, how to use it

Please make sure to plan the test as clearly as possible

TOPICS	Points
Pattern	It should cover use-case A, B, C on the application vendor is assigned to
Scenarios	Business patterns such as the to-be flow scenarios should be covered. Regular and irregular patterns should be considered
Data	Number of data on the data sheet should be covered
Logic	Check the logic in your app if it works or not
Performance test	Make sure to plan and conduct performance test that can ensure the (execution, connection, whether the simultaneous connections, load is bearable)
Method	Testing scenarios to be clearly stated on the methodology such as the mock app of android and iOS or through an online testing environment. The developed App should be usable for the PoC

About the test schedule

The test should be conducted in December 2024.



System-to-system linkage testing will be initiated by the app vendor, with Accenture supporting scenario and test case review and vendor-to-vendor test coordination.

	Vendors	Anticipated Roles
Implement	App Vendor	<ul style="list-style-type: none"> • Lead system connection test • Provide test plan and sample test data • Create test scenario • Implement test and confirm operation • Report test result
	Bhutan API/DB Vendor	<ul style="list-style-type: none"> • Create test scenarios and scripts related to data linkage between systems (apps) based on requirement definition documents and design documents • Confirm operation of API/DB functions according to test scenarios and scripts
	Accenture (Infra/Security)	<ul style="list-style-type: none"> • Create test scenarios and scripts related to data linkage between systems (apps) based on requirement definition documents and design documents • Confirm operation of Infra/Security functions according to test scenarios and scripts
Manage	RGoB (TWG)	<ul style="list-style-type: none"> • Confirm consistency between areas coordination among vendors
	Accenture (Strategy, PMU)	<ul style="list-style-type: none"> • Support for the test scenarios or requirement • Coordination of testing operations between vendors

S.No	Non-functional Requirements	Required in App? (Yes/No)	Availability in DHP (Yes/No)	Details
1 Matters regarding handover				
1.1	Handover to common operations management vendor and next application software maintenance vendor	Yes (Create a brief handover document)	Yes	<ul style="list-style-type: none"> Maintenance Operation - Scope of components for which maintenance during operation can be performed without stopping the system.
12 Matters related to education/training				
12.1	Basic requirements for education	Yes (for each use-case, need basic training material)	Yes	<ul style="list-style-type: none"> Information related to operational management training - This item relates to the implementation of operation training. User-specific training with clear explanation of implementation. (it will be done by PoC)

Non-functional Requirement for Health Service App

S.No	Non-functional Requirements	Required in App? (Yes/No)	Availability in DHP (Yes/No)	Details
13 Matters relating to Operations				
13.1	Common Requirements		Yes	<ul style="list-style-type: none"> Operations Architecture
13.2	Operational Management and Monitoring requirements	Yes (During the PoC period after development, including if there is a problem, the contact point 9 a.m. – 9 p.m. till the end of contact)	Yes	<ul style="list-style-type: none"> Operations Management – Scheduling, orchestration, Monitoring, configuration, logs
13.3	Evaluation and Improvement of Actual Operation	Yes (for recommendation to next development phase)	No	
13.4	Periodic Maintenance Requirements	Yes	Yes	<ul style="list-style-type: none"> Maintenance operations – planned system shutdown - This item concerns planned service outages performed in order to carry out system maintenance operations, such as inspections, region expansion, defragmentation, master data maintenance, and the like. Scheduled maintenance frequency
13.5	Maintenance System	Yes (how many people will be in support)		